SECOM Subject file

30 December 1977

MEMORANDUM FOR: Director, OPP
Director, OPEI
Chairman, COMIREX
Chairman, SIGINT Committee

FROM: [redacted] STAT
Acting Chairman, Security Committee

SUBJECT: Proposed Executive Order on
Security Classification

1. Attached is the final draft of the proposed Executive Order to state national policy on security classification. This draft reflects changes made at the direction of the PRM-29 Ad Hoc Committee co-chairmen to accommodate comments on the first formal draft. A number of those comments were received from the Congress (particularly from Rep. Preyer) and from public interest groups, as a result of the President's direction that the draft Order be made available to interested parties outside the Executive Branch. Handwritten changes to the attached draft were made by the White House staff during final coordination.

2. Your attention is invited particularly to the language in section 4(a) of the draft dealing with declassification policy. Its inclusion of a required balancing test for continuing classification beyond the initial authorized period (normally, 20 years) accords with suggestions from the DCI and from Rep. Preyer for such a test. The DCI's suggestion, however, was advanced with a view of trying to retain Executive Branch control over the subjective process of balancing national security interests against the public's right to know. The passive voice construction used in the draft would appear to put any party to litigation under the Freedom of Information Act on an equal footing with an agency head over the question of demonstrating where that balance lies.

SUBJECT: Proposed Executive Order on
Security Classification

3. Request any comments you may have on the attached, with supporting rationale, be provided this office as soon as possible but no later than 13 January, 1978.

STAT

Attachment
General Counsel, OMB letter of
27 December 1977 with attached
draft Executive Order on "National
Security Information"

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

GENERAL COUNSEL

December 27, 1977

Enclosed, in accordance with the provisions of Executive Order No. 11030, as amended, is a proposed Executive order entitled "National Security Information."

This proposed order is a revision of the version circulated for comment on September 13, 1977, and entitled "National Security Information and Material."

That draft order was revised after an extensive review of all the comments received. The revision is shorter, but generally structured in the same manner as the original draft. There are several substantive changes; therefore, our additional review is solicited.

On behalf of the Acting Director of the Office of Management and Budget, I would appreciate receiving any comments you may have concerning this revised proposed order. If you have any comments or objections they should be received no later than Friday, January 20, 1978.

Because this is a revision, it is anticipated that your review should not take as long as the review of the original draft; however, inquiries or comments may be submitted by telephone to Mr. Ronald A. Kienlen of this office (395-5600).

Sincerely,

William M. Nichols
William M. Nichols
General Counsel

Enclosure

EXECUTIVE ORDER

NATIONAL SECURITY INFORMATION

By virtue of the authority vested in me by the Constitution of the United States of America; in order to balance the public's right to government information with the need to protect some national security information from disclosure, it is hereby ordered as follows:

TABLE OF CONTENTS

Section 1. Definitions.

(a) "Agency" means any executive department, military department, Government corporation or independent establishment in the executive branch.

(b) "Classified information" is official information which has been determined by proper authority to require a degree of protection against unauthorized disclosure in the interest of national security and is so designated.

(c) "Foreign-originated information" means information which has been provided to the United States in confidence by a foreign government or international organization of governments (hereinafter referred to as "international organization"), or an official of either, or produced by the United States pursuant to a joint arrangement with a foreign government or an international organization.

(d) "Intelligence method" means any human, technological, or other method that is or may be used in the gathering or analysis of foreign intelligence or foreign counterintelligence and which would suffer reduced effectiveness if exposed.

(e) "Intelligence source" means any human, technological or other source from which foreign intelligence or foreign counter-intelligence is, has been or may be derived and which would suffer reduced effectiveness if exposed.

(f) "Official information or material" hereinafter referred to as "information" means that information which is owned by, produced for or by, or under the control of the United States Government.

Sec. 2. Original Classification.

(a) Classification Designation. Information which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of the three designations listed below:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause significant damage to the national security.

(b) General Policy.

(1) In deciding whether information requires classification pursuant to this Order, the classifying official shall consider both the public's need for the greatest possible access to information and the national security need to protect certain information.

(2) If the classifier has reasonable doubt which security classification designation is appropriate, or whether the information should be classified at all, he should designate the less restrictive treatment.

(c) Classification Requirements. Information shall not be classified unless an original classification authority determines both: (1) that the information falls into one or more of the criteria set forth in subsection (d) below which apply equally to all three authorized classification designations; and (2) that the disclosure of such information could reasonably be expected to cause at least significant damage to the national security. It is reasonable to expect that information provided in confidence by a foreign government or international organization would satisfy the above-mentioned second step.

(d) Classification Criteria. ~~The following criteria describe~~ Information ~~which~~ may not be considered for classification unless its disclosure could reasonably be expected to:

(1) Make the United States or its allies vulnerable to attack by a foreign power, or weaken the ability of the United States or its allies to conduct armed operations or defend themselves, or diminish the military or operational effectiveness of the United States' armed forces; or

(2) Lead to hostile political, economic, or military action against the United States or its allies by a foreign power; or

(3) Reveal, in whole or in part, the defense or foreign policy plans or posture of the United States or its allies; provide a foreign nation with information upon which to develop effective countermeasures to such plans or posture; weaken or nullify the effectiveness of a United States military, foreign intelligence, or foreign counterintelligence plan, operation, project, or activity of significance to the national security; or

(4) Aid a foreign nation to develop or improve its military capability; or

(5) Reveal, jeopardize, or compromise an intelligence source or method, ~~an analytical technique for the interpretation of intelligence data~~ or a cryptographic device or system; or

(6) Disclose to other nations or foreign groups that the United States has, or is capable of obtaining, certain information concerning those nations or groups without their knowledge or consent; or

(7) Deprive the United States of a diplomatic, military, scientific, engineering, technical, economic, or intelligence national security advantage; or

(8) Create or increase international tensions; cause or contribute to political or economic instability or civil disorder in a foreign country; or otherwise significantly impair our foreign relations; or

(9) Disclose or impair the position of the United States or its allies in international negotiations; or

(10) Disclose the identity of a confidential foreign source of the Department of State, or of a United States diplomatic or consular post; or

(11) Disclose information or material provided to the United States in confidence by a foreign government or international organization; or

(12) Significantly diminish the effectiveness of U.S. Government programs for safeguarding nuclear materials or facilities.

(e) Prohibitions.

(1) No information may be classified to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition or independent initiative.

(2) Basic scientific research information not directly related to the national security may not be classified.

(3) A product of independent research and development which does not incorporate or reveal classified information to which the producer or developer was given prior access shall not be classified under this Order until and unless the government acquires a proprietary interest in the information. However, this Order shall not be construed to impinge upon the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

(4) References to classified documents which individually, or in aggregate, do not disclose classified information may not be classified and may not be used as a basis for classification.

(5) Classification shall not be used to limit dissemination of information which is not classifiable under the provisions of this Order, or to prevent or delay the public release of such information.

(6) No document shall be classified after an Agency has received a request for such document under the Freedom of Information Act or the Declassification Requests provision of this Order [Section 4(g)], unless such document requires the protection authorized by this Order, and such classification is authorized personally, and in writing, by the head of the Agency concerned.

(7) Classification may not be restored to information already declassified and released under this and prior Orders.

(f) Classification Authority.

(1) Top Secret. The authority to originally classify information "Top Secret" may be exercised only by such officials as the President may designate by publication in the Federal Register, by the Agency heads listed below, and by officials so authorized in accordance with the provisions of subsection (4) below:

The Secretary of State

The Secretary of the Treasury

The Secretary of Defense

The Secretary of the Army

The Secretary of the Navy

The Secretary of the Air Force

The Attorney General of the United States

The Secretary of Energy

The Chairman, Nuclear Regulatory Commission

The Director, Arms Control and Disarmament Agency

The Director of Central Intelligence

The Administrator, National Aeronautics and Space Administration

The Administrator, General Services Administration (Delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office.)

(2) Secret. The authority to originally classify information "Secret" may be exercised only by such officials as the President may designate by publication in the Federal Register, by the Agency heads listed below, by officials who have "Top Secret" classification authority and by officials so authorized in accordance with the provisions of subsection (4):

The Secretary of Commerce

The Secretary of Transportation

The Administrator, Agency for International Development

The Director, International Communication Agency

(3) Confidential. The authority to originally classify information "Confidential" may be exercised only by such officials as the President may designate by publication in the Federal Register, by the Agency heads listed below, by officials who have "Top Secret" and "Secret" classification authority and by officials so authorized in accordance with subsection (4):

The President and Chairman, Export-Import Bank of the United States

The President and Chief Executive Officer, Overseas Private Investment Corporation

(4) Limitations on Delegation of Classification Authority.

(i) The authority for original Top Secret classification may be delegated by officials designated in writing by the President, and by the Agency heads listed in subsection (1) above only to principal subordinate officials whom the Agency heads determine in writing to have a frequent need to exercise such authority. Authority so delegated may not be redelegated.

(ii) Officials designated in writing by the President, the Agency heads listed in subsections (1), (2) and (3) above, and officials with Top Secret classification authority may delegate their assigned original "Secret" or "Confidential" authority only to those subordinates ~~who~~ whom they determine in writing to have frequent need to exercise such authority. Authority so delegated may not be redelegated.

(iii) All delegations of original classification authority shall be in writing by name or title of position held or as prescribed in directives implementing this Order.

(iv) Delegations of classification authority shall be held to an absolute minimum. Administrative convenience is not a valid basis for such delegations. Periodic review of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

(5) ~~The head of any Agency no~~ No Executive Branch employee without specifically granted original classification authority herein may ~~not~~ originally classify information under this Order

unless specifically authorized in writing by the President. Requests to the President for such authority shall be directed through the Information Security Oversight Office, established herein. Approval of such requests shall be published in the Federal Register.

(g) Exceptional Cases. When an employee of an Agency which does not have authority to originally classify, or a contractor of such an Agency, originates information which is believed to require classification, the person or contractor shall protect that information in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the Agency having primary interest in the subject matter and authority to classify, with a request that a determination be made as to classification. Such requests shall be acted upon in 30 days. Where such Agency cannot be identified, the information shall be sent to the Director of the Information Security Oversight Office.

(h) Limitation on Duration of Classification.

(1) All original classification authorities shall, at the time of original classification, set a date or event for automatic declassification of the information as early as national security considerations will permit. Except as permitted in paragraph (2) below, the date shall not exceed six years from the date of original classification.

(2) Only heads of agencies listed in Section 2(f) and officials with Top Secret classification authority designated pursuant to this Order may set a later date or event for automatic declassification or for review to decide whether the information can be declassified. This date or event shall be no more than twenty years from the date of original classification of the information, except that the date for review of foreign-originated information may be up to 30 years after original classification. For each such classification beyond six years, the reason for the longer period must be recorded. This reason must include an explanation why the classification will continue to meet the requirements of subsection 2(c) throughout the extended period.

(i) Identification and Marking.

(1) At the time of origination, each classified document shall show on its face: (i) the identity of the original classification authority;

(ii) the office of origin; (iii) the date of the document's origin; (iv) the date or event for declassification or review; and (v) one of the three classification designations defined herein. ~~[and (vi) the criteria or criterion for classification as specified in Section 2(d) of this Order]~~ When the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required. ~~[The originator's file copy of]~~ Any document classified for more than six years shall reflect the reason for the prolonged classification and the identity of the official who authorized it, in accordance with Section 2(h).* (stet)

(2) Markings such as "For Official Use Only" and "Limited Official Use" shall not be used to identify information requiring protection pursuant to this Order.

(3) Terms such as "Sensitive," "Conference," or "Agency" shall not be used in conjunction with classification designations prescribed by this Order; e.g., "Secret-Sensitive," "Agency Confidential," or "Conference Confidential."

(4) Each classified document shall, by marking or other means, clearly indicate which portions are classified, with the applicable classification designation, and which portions are not classified, in order to facilitate excerpting and other uses. Agency heads may seek a waiver of this requirement from the Director of the Information Security Oversight Office for limited classes of information. The Director of the Oversight Office may, for good cause, grant and revoke such a waiver.

(5) Classified information furnished to the United States by a foreign government or international organization shall either retain its original classification designation or be assigned a United States classification designation. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information.

(6) Classified documents which contain or reveal information which the originator has determined is subject to special dissemination and reproduction limitations shall be clearly marked so as to place the recipient on notice of the restrictions.

Section 3. Derivative Application of Markings.

(a) Original classification authority shall not be given to persons who only reproduce, extract or summarize classified information or who only apply to information classification markings derived from source material or as directed by a security classification guide. Persons who apply derivative classification markings shall (i) respect classifications assigned by originators; (ii) to the maximum extent practicable verify the current level of classification of the information prior to applying such markings; (iii) in accordance with subsections (b)-(e) below, carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings; (iv) identify on the newly created material the original classifier or other authority for the derivative classification markings applied by them. (Note: The directive implementing this Order will contain language providing for a single such identification for documents based on multiple classified sources.)

(b) New material which derives its classification from [Source] information classified on or after the effective date of this Order shall be marked with the date or event for declassification or the date for review assigned to the source information.

(c) Dates or events for automatic declassification of [Source] information (U.S. or foreign) assigned pursuant to previous Executive orders shall be carried forward when such dates or events call for declassification of the source information twenty years or less from its date of origin.

(d) Except as specified in subsection (e) below, new material which is classified on the basis of previously classified [Source] information which bears no date or event for declassification, or which is marked for declassification in excess of twenty years from date of origin, shall be marked with a date for review for declassification which shall be twenty years from the date of original classification of the source information.

(e) New material classified on the basis of previously classified foreign originated information which bears no date or event for declassification, or is marked with dates or events for declassification in excess of 30 years,

shall be marked with a date for review for declassification which shall be 30 years from the date of original classification of the foreign source information.

Section 4. Declassification.

(a) General Policy. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. When information is classified, decisions concerning declassification or review shall be based on the expected loss of the information's sensitivity with the passage of time, or an expected occurrence of an event which would make classification unnecessary. Whenever information is reviewed, it shall be declassified unless it can be demonstrated that: (1) disclosure would cause at least significant damage to the national security in spite of the passage of time; and (2) the damage to national security would ~~be of such gravity as to~~ outweigh the public interest in disclosure.

(b) Declassification Authority. The authority to declassify or downgrade information classified under this or prior Executive orders shall be exercised as follows:

(1) Classified information may be declassified or downgraded by the official who authorized the original classification, by a successor, or by a supervisory official of either.

(2) Agency heads named in Section 2(f) shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority. These officials shall also be authorized by the Agency heads to resolve conflicts or doubts regarding classification.

(3) The Director of the Information Security Oversight Office may declassify or downgrade information when the Director determines that its classification violates this Order and in the exercise of his appellate function pursuant to Section 4(g)(2). The Director shall promptly notify the affected Agency of such a decision. The decision shall take effect 20 working days after such notification unless during that time the head of the affected Agency appeals the decision to the President through the National Security Council.

(4) The provisions of this Order relating to the declassification of national security information shall also apply to agencies which, under the terms of this Order, do not have current authority to originally classify information, but which formerly had such authority under prior Executive orders.

(c) Authority Over Transferred Information.

(1) For classified information transferred in conjunction with a transfer of function pursuant to statute or Executive order -- not merely for storage purposes -- the receiving Agency shall be deemed to be the originating Agency for all purposes under this Order.

(2) For classified information not transferred in accordance with subsection (1) above, but originated in an Agency which has ceased to exist, each Agency in possession shall be deemed to be the originating Agency for all purposes under this Order. Such information may be declassified or downgraded by the Agency in possession after consulting with any other Agency having an interest in the subject matter.

(3) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the Information Security Oversight Office's directives, and Agency guidelines.

(4) After the termination of a Presidential administration, the Archivist of the United States shall have the authority to review and declassify or downgrade all information classified by the President, his White House staff, or committees or commissions appointed by him or others acting in his behalf. This authority shall be exercised only after consultation with the agencies having primary subject matter interest.

(d) Information Originally Classified Under This Order. Except as provided in subsection (f) below, information classified on or after the effective date of this Order shall be declassified or reviewed in accordance with the date or event set pursuant to Section 2(h). Information not marked with such a date or event shall be automatically declassified six years after its origination.

(e) Information Classified Under Prior Orders. Except as provided in subsection (f) below, information which was classified before the effective date of this Order and already marked with a date or event directing declassification in 20 years or less from date of origin, shall be automatically declassified in accordance with such date or event unless declassified earlier. Information not so marked shall be reviewed for declassification in accordance with subsections (g) and (h) below.

(f) Foreign Originated Information. Foreign originated information shall be exempt from the automatic declassification and 20 year systematic review provisions of this Section. Unless declassified earlier, such information shall be reviewed for declassification 30 years from its date of origin. Such reviews shall be in accordance with the provisions of Section 4(a) and with guidelines developed by Agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned.

(g) Declassification Requests.

(1) Except as provided in (2) below, information classified pursuant to this or prior Executive orders, shall be reviewed for possible declassification upon request of any member of the public or government employee or Agency, provided the request is specific enough for the Agency to locate the information with reasonable effort. Procedures for processing such requests and appeals from denials, on the basis of classification, shall accord with procedures established by agencies to implement the Freedom of Information Act.

(2) Information less than ten years old originated by the President or a President's White House staff or Committees or Commissions appointed by him or others acting in his behalf, or information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107a is exempted from the provisions of subsection (1) above. Such information over ten years old shall be subject to declassification review upon the request of a member of the public, a government employee or an Agency. Such requests and appeals of denials on the basis of classification shall be processed in accordance with procedures developed by the Archivist of the United States. Whenever the

Archivist denies an appeal of such a request, the decision may be appealed to the Director of the Information Security Oversight Office who may order declassification. In such cases, the Director of the Information Security Oversight Office shall promptly notify agencies with primary subject matter interest, which may follow the appeals process set forth in Section 4(b)(3).

(3) Requests for copies of classified documents originated by agencies of the executive branch, but in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107a, shall be referred by the Archivist to the Agency of origin for processing in accordance with subsection (1) above and for direct response to the requester. The Archivist shall inform requesters of such referrals.

(4) No Agency in possession of a document classified under the provisions of this Order may, in response to a request made under the Freedom of Information Act or the Declassification Requests provision of this Order for such document, refuse to confirm the existence of such document, unless the fact of its existence would itself be classifiable under this Order.

(h) Systematic Review.

(1) Classified information constituting permanently valuable records of the Government as defined by 44 U.S.C. 2103 shall be ~~Systematically~~ reviewed for declassification as it becomes 20 years old. Agency heads listed in Section 2(f) of this Order may extend classification beyond 20 years, but only in accordance with Sections 4(a) and 4(h)(2). This authority may not be delegated. When classification is extended beyond 20 years, a date for declassification or the next review no more than 10 years later shall be set and marked on the document. Subsequent reviews for declassification shall be set at no more than 10 year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of information.

(2) Within 180 days after the effective date of this Order, the Agency heads listed in Section 2(f) shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue guidelines for systematic review covering 20-year old classified

information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, cannot be automatically declassified but must be reviewed item-by-item to determine whether continued protection beyond 20 years is needed. All information not identified in these guidelines as requiring review shall be automatically declassified at the end of 20 years from the date of original classification. These guidelines shall be authorized for use by the Archivist of the United States and by Agencies having custody of the information.

Section 5. Downgrading. Information classified under this or prior Orders and marked for automatic downgrading is downgraded accordingly without notification to holders. Other information classified under this or prior Orders, may be assigned a lower classification designation by the originator or other officials authorized to downgrade or declassify when such downgrading serves a useful purpose. Notice of such downgrading shall be provided to holders of the information to the extent practicable.

Section 6. Safeguarding.

(a) General Controls.

(1) No person shall be given access to classified information unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of official duties.

(2) All classified information shall be conspicuously marked to put all persons on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions.

(3) Controls shall be established to assure that classified information is used, processed, stored, reproduced and transmitted only under conditions which will provide adequate protection and prevent access by unauthorized persons.

(4) Classified information no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions of Chapters 21 and 33 of Title 44 of the United States Code.

(5) Classified information disseminated outside the executive branch shall, in so far as possible, be given the same protection as that afforded within the executive branch.

(b) Reproduction Controls.

(1) Top Secret documents shall not be reproduced without the consent of the originating office, unless otherwise marked by the originating office.

(2) Reproduction of Secret and Confidential documents may be restricted by the originating office.

(3) Reproduced copies of classified documents are subject to the same accountability and controls as the originals.

(4) Records shall be maintained by all reproducing offices to show the number and distribution of reproduced copies of all Top Secret documents; all documents covered by special access programs distributed outside the originating agency; and all Secret and Confidential documents marked in accordance with Section 2(i)(6).

(5) Subsections (1) and (2) above shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproductions must be destroyed after they are used.

(c) Special Access Programs.

(1) Agency heads listed in Section 2(f)(1) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this or prior Orders. Such programs may only be created or continued by the Agency heads or, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence, personally and in writing. Classified information in such programs shall be declassified according to the provisions of Section 4. Special access programs may be created or continued only on the specific showing that:

(i) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(ii) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(iii) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

(2) All such special access programs shall automatically terminate every three years unless renewed in accordance with the procedures in this subsection.

(3) Within 180 days after the effective date of this Order, the Agency heads listed in Section 2(f)(1) shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in this subsection. Those Agency heads shall also establish and maintain a central list of all special access programs they create or continue. Those Agency heads and the Director of the Information Security Oversight Office shall have non-delegable access to all such lists.

(d) Access by Historical Researchers and Former Officials. The requirement in Section 6(a)(1) that access to classified information be granted only as is necessary for the performance of one's official duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; provided that the Agency with jurisdiction over the information:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to assure that classified information is not disclosed by the researcher or published without prior review, declassification and approval for public release;

(3) takes reasonable action to ensure that access is limited to specific categories of information over which that Agency has classification jurisdiction;

(4) limits the access granted to the person who occupied a policy-making position, to items which the person originated, reviewed, signed or received, while in public office.

Section 7. Implementation and Review. The National Security Council shall monitor the implementation of this Order and shall provide overall policy direction for the information security program.

(a) Oversight Office and Interagency Committee.

(1) Subject to the direction of the President and the National Security Council, the Information Security Oversight Office is established to assist the National Security Council in monitoring implementation of this Order. This Office shall be placed in the General Services Administration. It shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have authority to appoint a staff. The Director shall:

(i) oversee Agency actions to ensure compliance with this Order and implementing directives;

(ii) consider and take action on complaints and suggestions from persons within or without the Government with respect to the administration of the information security program, including appeals from denials of declassification requests pursuant to Section 4(g)(2);

(iii) exercise the authority to declassify information provided by Sections 4(b)(3) and 4(g)(2);

(iv) develop, in consultation with the agencies and, subject to the approval of the National Security Council, promulgate directives for the implementation of this Order which shall be binding on the agencies;

(v) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(vi) review all Agency implementing regulations and systematic review guidelines to ensure their consistency with the provisions of the Order. If the Director finds any regulation or guideline inconsistent with this Order, he may require it to be changed. The Agency head may appeal such a decision to the National Security Council, which shall have final decision-making authority.

(vii) exercise case-by-case classification authority and review requests for original classification authority in accordance with Section 2(f)(5);

(viii) have the authority to conduct on-site reviews of the information security program of each Agency which handles classified information and to require of each such Agency such reports, information, and other cooperation as necessary to fulfill the above responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected Agency head may deny access. In such a case, the Agency head shall report the decision and the reason to the National Security Council, which may overrule the decision.

(2) There is also established an Interagency Information Security Committee which shall be chaired by the Director of the Oversight Office and shall be comprised of representatives of the Secretaries of State, Defense, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council Staff, the Domestic Policy Staff, and the Archivist of the United States. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies. The Committee shall meet at the Chairman's call and shall advise the Chairman on implementation of this Order.

(b) Agencies with Original Classification Authority. Each Agency granted original classification authority pursuant to this Order shall:

(1) Prior to the effective date of this Order, submit to the Information Security Oversight Office a copy of the regulations and systematic review guidelines it adopts pursuant to this Order and implementing directives. Subsequent changes to Agency regulations and systematic review guidelines shall also be forwarded to the Oversight Office.

(2) Publish in the Federal Register those unclassified regulations and systematic review guidelines or changes thereto which affect the general public.

(3) Designate a senior Agency official to conduct an active oversight program to ensure effective implementation of this Order.

(4) Designate a senior Agency official to chair an Agency committee with authority to act on all suggestions and complaints with respect to the Agency's administration of the information security program.

(5) Establish a process to decide appeals from denials of declassification requests, pursuant to Section 4(g).

(6) Establish an on-going program to familiarize Agency personnel and others with access to classified information with the provisions of this Order and implementing directives. There shall also be established and maintained an active security orientation and education program for such personnel in order to impress upon each individual his or her responsibility for exercising vigilance and care in complying with the provisions of this Order and to encourage him or her to challenge classification decisions where they believe them to be improper.

(7) Ensure the preparation and promulgation of security classification guidance adequate to facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

(8) Develop and promulgate systematic review guidelines in accordance with Section 4(h)(2).

(9) Take necessary action to ensure that:

(i) a demonstrable need for access to classified information is established prior to the initiation of administrative clearance procedures, and

(ii) the number of people granted access to classified information is reduced to and maintained at the minimum, consistent with operational requirements and needs.

(10) Ensure that safeguarding practices are continuously reviewed and eliminate those which are duplicative or unnecessary.

(11) Submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

(c) Agencies without Original Classification Authority. Each Agency which has not been granted original classification authority but which handles classified information shall comply with subsections (b)(3), (4), (6), (9), (10) and (11) above.

Section 8. Administrative Sanctions.

(a) Any officer or employee of the United States who knowingly and willfully classifies or continues the classification of information in violation

of this Order or any implementing directive; or knowingly and willfully and without authorization, discloses ~~classified~~ properly classified under this Order information or compromises classified information through negligence; or knowingly and willfully violates any other provision of this Order or implementing directive which the head of an Agency determines to be a serious violation, shall be subject to appropriate administrative sanctions. In any case in which the Oversight Office finds that a violation has occurred, it shall make a report to the head of the Agency concerned so that corrective steps may be taken and appropriate sanctions imposed.

(b) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and Agency regulations.

(c) Agency heads shall make provision to ensure that appropriate and prompt corrective administrative action is taken whenever a violation under subsection (a) occurs and that both the Information Security Oversight Office and the Department of Justice are notified immediately of any case in which a violation of the criminal law may be involved.

Section 9. Atomic Energy Material. Nothing in this Order shall supersede any requirements made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of such Atomic Energy Act and the regulations of the Department of Energy under that Act.

Section 10. Interpretation of the Order. The Attorney General, upon request by the head of an Agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

Section 11. Revocation of Prior Orders and Directives. Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 [3 C.F.R. 1085 (1971-75 Comp.)] are revoked.

Section 12. Effective Date. This Order shall become effective on , except that the functions of the Information Security Oversight Office specified in Section 7(a)(1)(iv) and 7(a)(1)(vi) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee, established pursuant to Executive Order 11652.